Software Engineering Institute
Carnegie Mellon University

Defining a Progress Metric for CERT-RMM Improvement

Gregory Crabb
Nader Mehravari
David Tobar

September 2017

TECHNICAL NOTE
CMU/SEI-2017-TN-003

CERT Division

http://www.sei.cmu.edu

This material is based upon work funded and supported by the Independent Agency under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

This report was prepared for the SEI Administrative Agent AFLCMC/AZS 5 Eglin Street Hanscom AFB, MA 01731-2100

DM17-0306

Table of Contents

List of Figures

List of Tables

Acknowledgments

The United States Postal Service (USPS) Chief Information Security Officer (CISO) engaged the Software Engineering Institute (SEI) to support its cybersecurity and resilience improvement activities, including implementation of the CERT-Resilience Management Model (RMM), which led to the SEI's development of the Cybersecurity Program Progress Metric (CPPM). The authors acknowledge the contributions to the CPPM development by former SEI members Julia H. Allen and Pamela D. Curtis. The authors also acknowledge the USPS CISO organization for its feedback on the use of the CPPM.

Abstract

This report describes how the authors defined a Cybersecurity Program Progress Metric (CPPM) in support of a large, diverse U.S. national organization. The CPPM, based on the CERT-Resilience Management Model (CERT-RMM) v1.1, provides an indicator of progress towards achievement of CERT-RMM practices. The CPPM is an implementation metric that can be used to measure incremental progress in implementation of CERT-RMM practices and, through an aggregate score, show overall progress in achieving the goals of a cybersecurity program. The underlying concept of a CERT-RMM-based index is applicable to any organization using the CERT-RMM for model-based process improvement for such operational risk management activities as cybersecurity, business continuity, disaster recovery, IT operations, and incident response. Moreover, the underlying concept is applicable to other models such as the Cybersecurity Capability Maturity Model (C2M2).

1 Introduction

The purpose of this report is to describe a new metric, the Cybersecurity Program Progress Metric (CPPM), whose purpose is to provide a meaningful measure of progress towards implementing the CERT-Resilience Management Model (CERT-RMM) [Caralli 2011]. The metric measures progress in implementing a subset of CERT-RMM practices and achieves its maximum score when all selected CERT-RMM practices have been fully implemented. The organization using the CPPM decides which CERT-RMM practices to implement based on the organization's view of its risks and its long-term cybersecurity and resilience objectives and priorities.

Metrics are important for assessing the performance of ongoing cybersecurity operations and evaluating progress toward meeting cybersecurity objectives of the organization. By using a defined, repeatable process for calculating the CPPM, organizational leaders can confidently rely on it and its trend over time as a reliable indication of progress toward improving cybersecurity and resilience capabilities.

The underlying concept of a CERT-RMM-based index is applicable to any organization that is using the CERT-RMM for model-based process improvement for such operational risk management activities as cybersecurity, business continuity, disaster recovery, IT operations, and incident response. Moreover, the underlying concept is applicable to other models such as the Cybersecurity Capability Maturity Model (C2M2).

Section 2 provides a brief introduction to typical types of cybersecurity metrics, to place the CPPM into appropriate context. Section 3 covers existing metrics and scales specifically used with the CERT-RMM. Section 4 defines the CPPM in more detail as a CERT-RMM-based metric. Section 5 describes the use of the CPPM, including how it is calculated, and its advantages and disadvantages compared to other CERT-RMM metrics.

2 Types of Security Metrics

Metrics are extremely important in providing objective information and situational awareness to help in making better decisions. Metrics can allow an organization to judge how well its cybersecurity operations are performing and to objectively evaluate progress toward meeting its cybersecurity objectives. An organization can improve its operational effectiveness and accountability for it based on metrics. Additionally, the right metrics can provide quantifiable inputs for making defendable resource allocation decisions.

Technical metrics measure aspects of controls implemented through technology (systems, software, hardware, networks, and infrastructures) or technology performance. Examples include metrics for access controls, firewalls, encryption, intrusion detection systems, patch deployment, and antivirus.

Process metrics measure processes, a series of activities and tasks, that produce a work product or that lead to a particular outcome. The National Institute of Standards and Technology Special Publication 800-55 Revision 1, Performance Measurement Guide for Information Security [NIST 2008] describes three types of metrics:

- **Implementation metrics** measure progress in implementation of a security program/policy. These metrics answer questions such as the following:
  - Is this process, activity, or practice being performed and to what extent?
  - Are the improvement projects being executed according to plan?
  - Are the underlying cybersecurity practices being fully implemented and institutionalized across the enterprise?

These metrics help more with assessing compliance and less with how well the practice is being performed. An example of an implementation metric would be the percentage of users who have received anti-phishing training.

- **Effectiveness/efficiency metrics** measure whether security processes are implemented correctly, operating as intended, and meeting the desired outcome. They measure two aspects of implementation results: the robustness of the results itself, referred to as effectiveness, and the timeliness of the results, referred to as efficiency. These type of metrics answer questions such as the following:
  - How good is the work product or outcome of the process, activity, or practice?
  - Does it achieve the intended result?
  - Does it reduce cybersecurity risks?
  - How timely is the security process?

An example of an effectiveness metric would be a phishing click-rate comparison between users who have received relevant training and those who have not.

- **Impact metrics** articulate the impact of cybersecurity on an organization's business or mission. These metrics may answer questions such as the following:

  - What percentage of the organization's IT budget is devoted to cybersecurity and resilience?
  - What mission-related impacts has the information security program produced?
- An additional type of metric, particularly relevant to the use of the CERT Resilience Management Model and other process improvement models, is the **process performance metric**, which can help organizations plan, predict, and control a process, and therefore can lead to the ability to manage and improve the process. An example of a process performance metric would be average incident resolution time per month.

Generally, an organization will need to focus first on implementation metrics, as a program moves towards implementation. Eventually, as a program is more fully implemented, effectiveness/efficiency metrics and process performance metrics become more useful. Implementation and effectiveness/efficiency metrics are complementary, and it is often useful to have metrics of both types.

The CPPM metric represents progress in implementing a selected subset of CERT-RMM practices and is therefore an implementation metric.

3 Existing Scales and Metrics used with the CERT-RMM

One basis for establishing an organization's long-term cybersecurity and resilience goals is the CERT-RMM. This model is a comprehensive, structured, process improvement body of knowledge for managing cybersecurity and other domains that address the resilience of organizations. Given the success in applying the CERT-RMM model to a wide range of diverse organizations and projects, an organization can confidently use the CERT-RMM as an overarching framework to establish cybersecurity and resilience goals and inform and organize organizational activities.

The CERT-RMM organizes its practices into a scale of maturity levels (CMMI-type capability levels 0, 1, 2, and 3) as described in the CERT-RMM book [Caralli 2011]. (See Figure 1.) These maturity levels are based on measures of process institutionalization as a key factor in institutionalizing operational resilience.

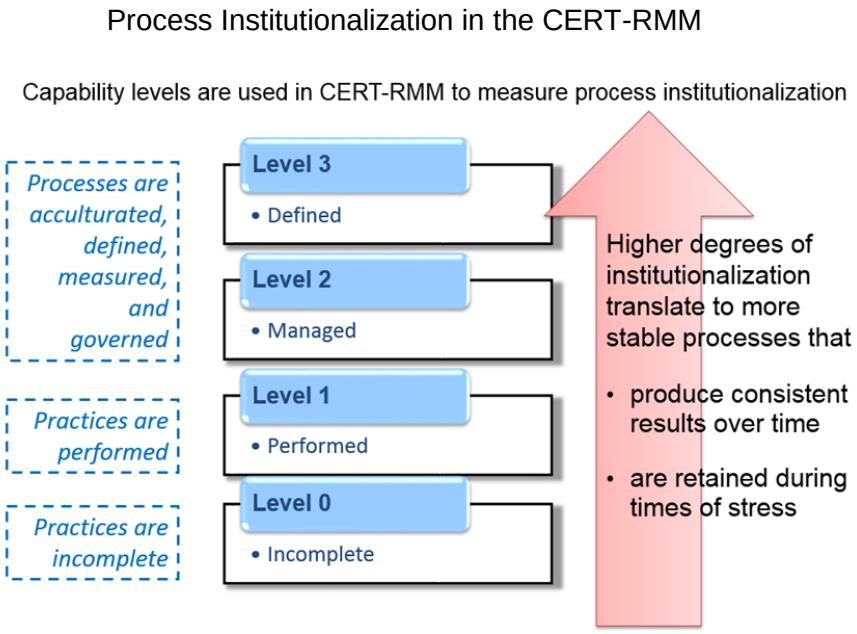

Figure 1: CERT-RMM Maturity Levels

In addition to this CERT-RMM scale, the SEI and others have used other scales with the CERT-RMM and its derivatives. These other scales include the seven-level CERT-RMM Maturity Indicator Level scale (MIL 0 to MIL 6) introduced in an SEI technical note [Butkovic 2013], the four-level scale (MIL 0 to MIL 3) used in the Cybersecurity Capability Maturity Model [DOE 2014], and the six-level scale (MIL 0 to MIL 5) used in Cyber Resilience Review [DHS 2016].

These scales are similar in that they provide a maturity level rating for the assessed organization's process areas. The CPPM differs from these maturity scales. The CPPM provides an overall score that reflects the extent of implementation of CERT-RMM practices and is indicative of maturity but does not necessarily reflect a fully reached maturity level. The CPPM is very useful in tracking overall progress over time.

4 CPPM Description

The CPPM metric is based on the aggregate scoring of selected CERT-RMM practices. Typically an organization will not implement the entirety of CERT-RMM practices, but rather it will decide to implement a subset of CERT-RMM practices chosen to achieve its mission, strategic objectives, and priorities. The first step in defining an instantiation of the CPPM is to scope the metric to include scoring only for the selected CERT-RMM practices and to exclude scoring for practices not selected.

The CPPM is then calculated by scoring each selected practice, depending on the level of its instantiation, and aggregating the scores for a total CPPM score. Implementation status of CERT-RMM practices is assessed as being either Fully Implemented (FI), Largely Implemented (LI), Partially Implemented (PI), or Not Implemented (NI), described as FILIPINI scoring. Each of these levels has an associated numerical scoring value as shown in Table 1.

Table 1: Completion Levels and Values

Range of Completion Percentage	FILIPINI Scale	Associated Numerical Value
86-100% complete	FI Fully Implemented	3
51-85% complete	LI Largely Implemented	2
16-50% complete	PI Partially Implemented	1
0-15% complete	NI Not Implemented	0

The CPPM allows for tailoring in two areas:

- flexibility to use different weights for more difficult practices. A weighting factor of 1, 2, or 3 can be used for each practice to represent the degree of difficulty to implement that practice so that more complicated CERT-RMM practices are given more weight. The intent of this is to give more importance in the calculation of the CPPM to those practices that are more difficult to implement.
- normalization. The final aggregate score may be normalized as desired by the organization so that the maximum achievable score if all selected practices were fully accomplished would equal 100, 100%, 1,000 (or some other number if one is concerned about potential psychological disadvantage of normalizing to 100% because it may be interpreted as “perfection”).

Practice status may be assessed based on percentage complete or completion of significant activities or subpractice requirements. Assessed scoring values for each CERT-RMM practice can be entered into a scoring spreadsheet, enabling calculation of the value of the overall CPPM metric.

Table 2 provides a segment of a scoring spreadsheet showing examples of practice weights and current scores based on level of practice completion.

Table 2: Segment of Scoring Spreadsheet

RMM Process Areas	RMM Practices	RMM Practice Title	Typical Work Products	RMM Practice Weight (1,2,3)	Current Level of Practice Completion (FI=3, LI=2, PI=1, NI=0)
Asset Definition and Management	ADM:SG1.SP1	Inventory Assets	1. Asset inventory (of all high-value assets of each type) 2. Asset databases	1	1
Asset Definition and Management	ADM:SG1.SP2	Establish a Common Understanding	1. Asset profiles (for all high-value assets of each type) 2. Updated asset database (including asset profiles)	1	0
Asset Definition and Management	ADM:SG1.SP3	Establish Ownership and Custodianship	1. Owner identification 2. Custodian identification 3. Updated asset profiles (including owner and custodian) 4. Updated asset database (including owner and custodian)	1	0
Asset Definition and Management	ADM:SG2.SP1	Associate Assets with Services	1. List of high-value services and associated assets 2. Updated asset profiles (including service information) 3. Updated asset database (including service information)	2	0
Asset Definition and Management	ADM:SG2.SP2	Analyze Asset-Service Dependencies	1. List of potential conflicts due to asset dependencies 2. Mitigation actions and resolutions	2	0

Note: Not all columns of the scoring spreadsheet are shown in the sample above.

5 CPPM Considerations

5.1 Benefits of the CPPM

The value of the CPPM metric represents the extent to which current efforts are implementing selected CERT-RMM practices, and in this way are helping to achieve the organization's long-term goals. The CPPM provides a consistent methodology to calculate progress over time in implementing a comprehensive improvement program. The trend of the metric (up, down, or no change) over time is initially more important than the specific value of the metric. A simple spreadsheet can suffice to keep track of individual practice scores and to calculate the overall CPPM score.

In the CERT-RMM model, one cannot take credit for having achieved a practice at a higher level without having implemented all practices at the lower maturity level. One facet of the CPPM scoring is that it assigns value to achieving higher Maturity Level 2 and Level 3 practices regardless of whether all practices at lower levels have been fully implemented. The effect of this is to enable an organization to gain credit for achieving higher maturity CERT-RMM practices even when lower levels have not been fully reached. This is a valuable characteristic in enabling risk-based decisions over which practices to implement, given that an organization's requirements and priorities may not correspond to strictly defined maturity levels.

The CPPM, in giving partial credit as practices are implemented, is very useful in tracking overall progress and increments of progress, over time, which is particularly helpful when starting from a low level of maturity. The CPPM makes small improvements clearly visible, which serves as an incentive for organizations to make improvements (compared to a maturity scale of MIL 0 to MIL 5, which does not give partial credit and therefore does not reflect small improvements).

5.2 CPPM Implementation

One important concern is that the staff may come to drive its behavior based on improving the metric score, rather than on a fully reasoned and logically sequenced plan of action. Staff may seek to gain metric points by implementing practices that should logically only be implemented after lower level CERT-RMM-specific practices are completed. This type of behavior should be discouraged by ensuring efforts and actions are in keeping with well-thought-out improvement plans.

In addition to implementing the CERT-RMM and tracking progress via the CPPM, which are significant steps towards improving an organization's cybersecurity and resilience posture, we would also recommend the organization (or its CISO) identify and calculate other selected CERT-RMM metrics that are indicative of the performance and effectiveness of the cybersecurity program. This is important because although the CPPM reflects progress of implementation of CERT-RMM practices, it is not necessarily a complete indication of security posture, i.e., the extent to which the organization is secure and the extent to which the organization is likely to experience reduced impact during the next major cybersecurity incident.

Those calculating, interpreting, and using the CPPM should also take the following points into account:

- Training in the CERT-RMM will be important for both the staff implementing the improvement effort as well as the staff assessing progress.
- The organization may want to establish guidelines for the completion levels (FI, LI, PI, and NI) to try to ensure consistency in their use as an indicator of status. When applicable, the percentage complete levels (Table 1) should be used along with clear guidance on what is to be measured, to avoid subjective interpretations by different project managers. In some cases completion levels will be based on completion of significant activities. Diligence should be taken to ensure that guidelines for determining level of completion remain consistent.
- The organization should exercise diligence in carefully reviewing, analyzing, and questioning, where necessary, the completion levels. For example, the organization should consistently verify and assign completion level by using a list of typical work products for each CERT-RMM practice. Project managers should be trained to help the organization improve the accuracy and consistency of its reporting over time.
- It would also be a good idea to perform assessments when CERT-RMM process areas are near full implementation, and after that periodically or if problems arise.

6 Summary

The CPPM is an implementation metric that can be used to measure incremental progress in implementation of CERT-RMM practices and, through an aggregate score, show overall progress in achieving the goals of a cybersecurity program. The United States Postal Service (USPS) CISO organization is using the CERT-RMM along with the CPPM to help define and drive its cybersecurity and resilience improvement efforts. The USPS has used the CPPM metric to baseline, establish long-term goals, and measure progress on a regular basis. The metric is used at both the management level to drive improvement initiatives and at the executive level to brief USPS leadership on progress.

References

URLs are valid as of the publication date of this document.

[Butkovic 2013]
Butkovic, Matthew J. & Caralli, Richard A. *Advancing Cybersecurity Capability Measurement Using the CERT-RMM Maturity Indicator Level Scale* (CMU/SEI-2013-TN-028). Software Engineering Institute, Carnegie Mellon University. 2013.
http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=69187

[Caralli 2011]
Caralli, R. A.; Allen, J. H.; & White, D. W. *CERT Resilience Management Model: A Maturity Model for Managing Operational Resilience (CERT-RMM Version 1.1).* Addison-Wesley. 2011.
http://www.mypearsonstore.com/bookstore/cert-resilience-management-model-certrmm-a-maturity-0134609301

[DHS 2016]
Department of Homeland Security & Software Engineering Institute. *Cyber Resilience Review (CRR): Method Description and Self-Assessment User Guide.* Department of Homeland Security. 2016.
https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-method-description-and-user-guide.pdf

[DOE 2014]
Department of Energy & Department of Homeland Security. *Cybersecurity Capability Maturity Model (C2M2) Version 1.1*. Department of Energy. 2014.
https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf

[NIST 2008]
Chew, E.; Swanson M.; Stine, K.; Bartol, N.; Brown, A.; & Robinson, W. *Performance Measurement Guide for Information Security*. (NIST Special Publication 800-55 Revision 1). National Institute of Standards and Technology. 2008.
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	September 2017	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Defining a Progress Metric for CERT-RMM Improvement	FA8721-05-C-0003

6. AUTHOR(S)
Gregory Crabb
Nader Mehravari
David Tobar

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2017-TN-003

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116	n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

This report describes how the authors defined a Cybersecurity Program Progress Metric (CPPM) in support of a large, diverse U.S. national organization. The CPPM, based on the CERT-Resilience Management Model (CERT-RMM) v1.1, provides an indicator of progress towards achievement of CERT-RMM practices. The CPPM is an implementation metric that can be used to measure incremental progress in implementation of CERT-RMM practices and, through an aggregate score, show overall progress in achieving the goals of a cybersecurity program. The underlying concept of a CERT-RMM-based index is applicable to any organization using the CERT-RMM for model-based process improvement for such operational risk management activities as cybersecurity, business continuity, disaster recovery, IT operations, and incident response. Moreover, the underlying concept is applicable to other models such as the Cybersecurity Capability Maturity Model (C2M2).

14. SUBJECT TERMS	15. NUMBER OF PAGES
Security metrics, Resilience Metrics, CERT-Resilience Management Model (CERT-RMM), Cybersecurity Program Progress Metric (CPPM), United States Postal Service	19

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL